Citrix® MetaFrame XP® Security Standards and Deployment Scenarios

Including Common Criteria Information

MetaFrame XP Server for Windows with Feature Release 3

Citrix Systems, Inc.

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Citrix Systems, Inc.

Citrix, ICA (Independent Computing Architecture), MetaFrame, MetaFrame XP, NFuse and Program Neighborhood are registered trademarks, and Citrix Solutions Network and SpeedScreen are trademarks of Citrix Systems, Inc. in the United States and other countries.

Apple, LaserWriter, Mac, Macintosh, Mac OS, and Power Mac are registered trademarks or trademarks of Apple Computer Inc.

Java, Sun, and SunOS are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. Solaris is a registered trademark of Sun Microsystems, Inc. Sun Microsystems, Inc has not tested or approved this product.

Microsoft, MS-DOS, Windows, Windows NT, Win32, Outlook, ActiveX, and Active Directory are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries. Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corp. in the U.S. and other countries.

UNIX is a registered trademark of The Open Group.

All other trademarks and registered trademarks are the property of their owners.

Last Updated: June 1, 2004 5:39 pm (AM)

Contents

Introduction

About this White Paper

Citrix products offer the security specialist a wide range of features for securing a Citrix MetaFrame XP system.

When deploying Citrix MetaFrame XP Server for Windows with Feature Release 3 within U.S. federal government environments, security standards are an important consideration. This white paper addresses common issues related to such environments and the Federal Information Processing Standard 140 (FIPS 140).

This white paper provides an overview of the process of securing communications across a range of deployment models. Details of the individual security features are explained in the relevant product documentation. Although the document concentrates on U.S. Federal government and FIPS 140 requirements, the information is also useful for other government departments and organizations.

Target Audience

This white paper is designed to meet the needs of security specialists, systems integrators, and consultants working with U.S. government organizations.

Finding More Information

For assistance with securing a MetaFrame XP deployment, the following documentation is available on the product CD and from the Knowledge Center available on http://www.citrix.com/. To find the Knowledge Center, go to the Support and Services area of the Citrix Web site.

On your MetaFrame XP with Feature Release 3 CD and on the Citrix Web site Knowledge Center:

> The *Citrix MetaFrame XP Server Administrator's Guide* for Feature Release 3 explains how to install and configure MetaFrame XP on Windows servers. Included in this documentation is information about publishing applications, configuring the Citrix XML Service, and configuring the Citrix SSL Relay to provide TLS/SSL based communications.

On your MetaFrame XP Components CD and on the Citrix Web site Knowledge Center:

- The *Web Interface Administrator's Guide* explains how to install and configure the Web Interface and provides information about securing Web Interface deployments using TLS/SSL based communications.
- The *Secure Gateway Version 2.0 Administrator's Guide* explains how to install and configure Secure Gateway to provide a secure Internet gateway for ICA traffic traveling into and out of a MetaFrame server farm.
- The *Citrix ICA Win32, Version 7.0, Client Administrator's Guide* explains how to install, configure, and deploy Citrix ICA Clients for Win32. The guide includes a chapter about ICA Client security measures and features.

What’s New

A number of security features and enhancements are implemented in Citrix MetaFrame XP Server for Windows with Feature Release 3. These enhancements include:

Web Interface Microsoft Secure Channel support. The Web Interface for MetaFrame XP uses Microsoft's secure channel (Schannel) security protocol on Windows platforms. This protocol can use cryptographic modules that are FIPS 140 validated.

Note NFuse Classic has been integrated as a feature in MetaFrame XP. NFuse Classic is now called the Web Interface for MetaFrame XP.

Certificate revocation checking. ICA Clients for Windows (Program Neighborhood, Program Neighborhood Agent, and ICA Web Client for Win32) now support certificate revocation checking. This is supported only by ICA Clients running on Windows 2000 and Windows XP.

Windows Server 2003 support. MetaFrame XP is now available for Windows Server 2003.

Common Criteria Evaluation. MetaFrame XP Presentation Server for Windows, Feature Release 3 with Hotfix MPS_FR3_EAL2, was evaluated and meets Common Criteria Evaluation Assurance Level EAL2. See “Common Criteria” on page 9.

Note MetaFrame XP Server for Windows is synonymous with MetaFrame XP Presentation Server for Windows as appears in Common Criteria documentation.

Security Considerations in a MetaFrame XP Deployment

MetaFrame XP provides server-based computing to local and remote users through the Independent Computing Architecture (ICA) developed by Citrix.

ICA is the foundation of Citrix server-based computing with MetaFrame XP and ICA Client software. In simplified terms, the ICA protocol transports an application's screens (and audio where relevant) from a MetaFrame XP server to ICA Client users, and returns the users' input to the application on the server.

As an application runs on a MetaFrame XP server, MetaFrame XP intercepts the application's display data and uses the ICA protocol to send this data (on standard network protocols) to the ICA Client software running on the user's client device. When the user types on the keyboard or moves and clicks the mouse, the ICA Client sends this data to the application on the MetaFrame XP server.

The Citrix ICA protocol provides advanced capabilities and enhanced performance with Windows terminal services. ICA delivers high performance on high- and low-bandwidth connections. ICA requires minimal client workstation capabilities and includes error detection and recovery, encryption, and data compression.

In a MetaFrame XP deployment including the Web Interface, communication is conducted using both the ICA and HTTP protocols, among three different points: the MetaFrame XP server, a server running the Web Interface, and a client device with a Web browser and ICA Client.

In a MetaFrame XP deployment, you can configure encryption using either:

- Citrix SSL Relay
- Secure Gateway

The Citrix SSL Relay component is integrated into MetaFrame XP. The Secure Gateway is provided on the MetaFrame XP Components CD.

Common Criteria

Common Criteria (CC) certification is an internationally recognized standard for evaluating the security of IT products and systems. CC certification provides assurance that products were thoroughly and independently tested and validated against a set of requirements established by the worldwide International Standards Organization to ensure IT security.

For customers, especially US federal and international government agencies, CC certification is an important requirement when procuring IT products and systems. CC certification is also applicable to private sector industries such as healthcare and financial.

Citrix MetaFrame XP Presentation Server for Windows, Feature Release 3 with Hotfix MPS_FR3_EAL2, was evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL2.

For further details, see www.citrix.com (select **About Citrix** > **Legal** > **Common Criteria**). The following documents are available on the Web site:

- *Security Target for Citrix MetaFrame XP Presentation Server for Windows with Feature Release 3*

  This document specifies the functional, environmental, and assurance evaluation requirements.

- *Common Criteria Evaluated Configuration Guide, Citrix MetaFrame XP Server for Windows With Feature Release 3*

  This document describes the requirements and procedures for installing and configuring MetaFrame XP in accordance with the Common Criteria (CC) evaluated deployment.

  The Common Criteria evaluated configuration is similar to sample deployment B.2 shown on page 22.

- *Common Criteria Certification Report No. P201, Citrix MetaFrame XP Presentation Server for Windows, Feature Release 3, with hotfix MPS_FR3_EAL2*

  The Certification Report, prepared by the certification body (UK IT Security Evaluation and Certification Scheme Certification Body, CESG), states the outcome of the Common Criteria security evaluation.

FIPS 140 and Citrix MetaFrame XP

Federal Information Processing Standard 140 (FIPS 140) is a U.S. federal government standard that details a benchmark for implementing cryptographic software. It provides best practices for using cryptographic algorithms, managing key elements and data buffers, and interacting with the operating system. An evaluation process that is administered by the National Institute of Standards and Technology's (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) allows encryption product vendors to demonstrate the extent to which they comply with the standard, and thus, the trustworthiness of their implementation.

Some U.S. government organizations restrict purchases of products that contain cryptography to those that have FIPS 140 validated modules. To facilitate implementing secure application server access and to meet the FIPS 140 requirements, Citrix products can use cryptographic modules that are FIPS 140 validated in Windows 32-bit implementation of secure SSL/TLS connections. The security community at large values products that follow the guidelines detailed in FIPS 140 and the use of FIPS 140 validated cryptographic modules.

With the release of MetaFrame XP Server for Windows with Feature Release 3, the following components can use cryptographic modules that are FIPS 140 validated:

- Citrix ICA Clients for Win32: Program Neighborhood, Program Neighborhood Agent, and the ICA Web Client for Win32
- Secure Gateway for Windows
- Citrix MetaFrame XP Server for Windows with Feature Release 3
- SSL Relay
- Web Interface for MetaFrame XP with Feature Release 3

When using the client and server components listed above with the SSL/TLS connection enabled, the cryptographic modules that are used are FIPS 140 validated. The cryptographic modules used are those provided by the Microsoft Windows operating system.

For details about these specific modules, visit the Microsoft Web site: http://www.microsoft.com/technet/security/issues/fipssum.asp.

For a listing of FIPS 140 validated modules, refer to the NIST Web site to view a list of the currently validated modules: http://csrc.nist.gov/cryptval/140-1/1401val.htm.

For additional details regarding FIPS 140 and NIST, visit the NIST site: http://csrc.nist.gov/cryptval/.

TLS/SSL

Secure Socket Layer (SSL) is an open, nonproprietary protocol that provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. Where SSL is used to secure communications between clients and your MetaFrame XP servers, the Citrix SSL Relay is required at each MetaFrame XP server within each farm, or you can use the Secure Gateway. Both solutions are discussed in this document.

Transport Layer Security (TLS) is the latest, standardized version of the SSL protocol. TLS is an open standard and like SSL, TLS provides server authentication, encryption of the data stream, and message integrity checks. The Citrix SSL Relay, described above, supports TLS and you can configure the SSL Relay, the Secure Gateway, and the Web Interface to use TLS. Support for TLS Version 1.0 is included in MetaFrame XP Server for Windows with Feature Release 3.

Because there are only minor differences between SSL and TLS, the server certificates in your MetaFrame XP installation can be used for both SSL and TLS purposes.

Government Ciphersuites

You can configure MetaFrame XP Server for Windows with Feature Release 3, the Web Interface, and the Secure Gateway to use government-approved cryptography to protect “sensitive but unclassified” data. The government ciphersuite is RSA_WITH_3DES_EDE_CBC_SHA.

IPSec

IP Security (IPSec) is a set of standard extensions to the Internet Protocol (IP) that provides authenticated and encrypted communications with data integrity and replay protection. IPSec is a network-layer protocol set, so higher level protocols such as Citrix ICA can use it without modification.

Although such deployment scenarios are not within the scope of this document, you can use IPSec to secure a MetaFrame XP deployment within a Virtual Private Network (VPN) environment.

IPSec is described in Internet RFC 2401.

Microsoft Windows 2000 (and later releases) has built-in support for IPSec.

Smart Cards

You can use smart cards with MetaFrame XP Server for Windows with Feature Release 3, supported ICA Clients, and the Web Interface to provide secure access to applications and data. Using smart cards with MetaFrame XP and the ICA Clients simplifies the authentication process while enhancing logon security. MetaFrame XP supports smart card authentication to published applications, including “smart card enabled” applications such as Microsoft Outlook.

In a business network, smart cards are an effective implementation of public-key technology and can be used to:

- Authenticate users to networks and computers
- Secure channel communications over a network
- Use digital signatures for securing content

If you are using smart cards for secure network authentication, your users can authenticate to applications and content published on MetaFrame XP servers. In addition, smart card functionality within these published applications is also supported.

For example, a published Microsoft Outlook application can be configured to require that users insert a smart card into a smart card reader attached to the client device to log on to the MetaFrame XP server. After users are authenticated to the application, they can digitally sign email using certificates stored on their smart cards.

Citrix supports the use of Personal Computer Smart Card (PC/SC) based cryptographic smart cards. These cards include support for cryptographic operations such as digital signatures and encryption. Cryptographic cards are designed to allow secure storage of private keys such as those used in Public Key Infrastructure (PKI) security systems. These cards perform the actual cryptographic functions on the smart card itself, meaning the private key and digital certificates never leave the card. In addition, you can use two-factor authentication for increased security. Instead of merely presenting the smart card (one factor) to conduct a transaction, a user-defined PIN (a second factor), known only to the user, is used to prove that the cardholder is the rightful owner of the smart card.

ICA Clients

Users access applications running on MetaFrame XP servers using ICA Client software installed on their client devices. ICA lets virtually any type of client device access applications over any type of network connection, including LAN, WAN, dial-up, and direct asynchronous connections. Because ICA does not download applications to client devices (as in the Network Computing architecture), application performance is not limited by bandwidth or device performance.

ICA Clients are available for Windows, Macintosh, UNIX, Linux, EPOC, Windows CE, DOS, and Java operating systems. Additionally, the ICA Web Client can be used with Web browsers that support ActiveX controls or Netscape plug-ins.

As described earlier, ICA Clients for Win32 use cryptographic modules provided by the Microsoft Windows operating system. Other ICA Clients, including the ICA Client for Java, contain their own cryptographic modules. The ICA Client for Java can therefore be used on older Microsoft Windows operating systems that are not upgraded to support strong encryption.

The following table lists the available ICA Clients and details whether or not the ICA Client is FIPS 140 compliant, supports TLS, includes smart card support, uses government ciphersuites, and supports certificate revocation checking. Note that certificate revocation checking is applicable to ICA Clients running on Windows 2000 and Windows XP only.

Note ICA Clients not listed in the table do not support any of the security features listed below.

	FIPS 140	TLS Support	Government Ciphersuite	Certificate Revocation Checking	Smart Card Support
Program Neighborhood (ICA Client for WIn32) Version 7.0	▶	▶	▶	▶	▶
Program Neighborhood Agent (ICA Client for WIn32) Version 7.0	▶	▶	▶	▶	▶
ICA Web Client for Win32 Version 7.0	▶	▶	▶	▶	▶
ICA Client for Windows CE WBT Version 7.0		▶	▶		▶
ICA Client for Pocket PC Version 7.0		▶	▶		
ICA Client for Java Version 7.0		▶	▶		
ICA Client for Mac OS X Version 6.30		▶			
ICA Client for Win16 Version 6.20					
ICA Client for Linux Version 7.0		▶	▶		▶
ICA Client for Solaris SPARC Version 6.30		▶			▶
ICA Client for UNIX (IBM AIX) Version 6.30		▶			▶
ICA Client for UNIX (SGI IRIX) Version 6.0					
ICA Client for UNIX (HP-UX) Version 6.30		▶			
ICA Client for OS/2 Version 6.012					
ICA Client for EPOC Version 1 and 2					

Certificates

The table below details the maximum certificate key lengths and the certificate source for the FIPS 140 compliant ICA Clients.

	Max Certificate Key Length (OS or bits)	Root Certificate Source (OS or ICA Client)
Program Neighborhood (ICA Client for WIn32) Version 7.0	OS	OS
Program Neighborhood Agent (ICA Client for WIn32) Version 7.0	OS	OS
ICA Web Client for Win32 Version 7.0	OS	OS
ICA Client for Windows CE WBT Client Version 7.0	2048	ICA Client
ICA Client for Pocket PC Version 7.0	2048	ICA Client
ICA Client for Java Version 7.0	2048	ICA Client
ICA Client for Mac OS X Version 6.30	2048	ICA Client
ICA Client for Linux Version 7.0	2048	ICA Client
ICA Client for Solaris SPARC Version 6.30	2048	ICA Client
ICA Client for UNIX (IBM AIX) Version 6.30	2048	ICA Client
ICA Client for UNIX (HP-UX) Version 6.30	2048	ICA Client

Maximum Certificate Key Length (bits). The table shows the maximum certificate key length for ICA Clients. For ICA Clients marked with OS, the maximum certificate key length is determined by the cryptographic module service provider and the operating system.

Certificate Source. The table details the certificate source for each ICA Client. ICA Clients marked with OS use certificates stored in the operating system certificate store. ICA Clients marked with ICA Client use certificates bundled with the ICA Client. Citrix ICA Clients include native support for the following certificate authorities:

- VeriSign, Inc., http://www.verisign.com
- Baltimore Technologies, http://www.baltimore.com

Government organizations may use a different certificate authority. If so, you must install the root certificate for the certificate authority on each client device.

Additional MetaFrame XP Security Features

The following MetaFrame XP security features are supported. However, they are not discussed in this document and are not included in any of the example deployment scenarios. For details concerning these features, see the relevant product documentation.

Web Interface RSA SecurID authentication

RSA SecurID can be used as an authentication method for the Web Interface running on Windows servers. If enabled, users must log on using their credentials (user name, password, and domain) plus their PASSCODE. The PASSCODE comprises a PIN (Personal Identification Number) followed by the RSA SecurID tokencode (the number displayed on the RSA SecurID token).

ICA Encryption (SecureICA)

ICA Encryption (SecureICA) is integrated into MetaFrame XP. You can use ICA Encryption (128-bit) to protect the information sent between a MetaFrame XP server and an ICA Client.

ICA Encryption does not use FIPS 140 compliant algorithms. You can configure ICA Clients and MetaFrame XP Servers to avoid using ICA Encryption.

Sample Deployments

Both Citrix SSL Relay and Secure Gateway are capable of supporting TLS-based and SSL-based encryption and selection is largely a matter of deciding which topology best meets the needs of the organization’s security policies. Each approach has its own advantages and the relative merits of the two are best illustrated by considering the following sample deployment models:

Sample Deployment A. Using Citrix SSL Relay to provide end-to-end TLS/SSL encryption between a specific MetaFrame XP server and an ICA Client.

Sample Deployment B. Using Secure Gateway in the Single-Hop deployment to provide TLS/SSL encryption between a secure Internet gateway server and an SSL-enabled ICA Client, combined with encryption of the HTTP communication between the Web browser and the Web server. Additionally, you can secure ICA traffic within the internal network using IPSec.

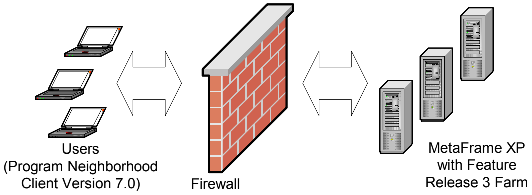
The Common Criteria evaluated configuration is similar to sample deployment B.2 shown on page 22. For further details concerning the evaluated configuration, see the *Common Criteria Evaluated Configuration Guide, Citrix MetaFrame XP Server for Windows With Feature Release 3*.

Sample Deployment C. Using Secure Gateway in the Double-Hop deployment to provide TLS/SSL encryption between a secure Internet gateway server and an SSL-enabled ICA Client, combined with encryption of the HTTP communication between the Web browser, Web Interface, and Secure Gateway Proxy. Additionally, you can secure ICA traffic within the internal network using IPSec.

Sample Deployment D. Using SSL Relay with the Web Interface to encrypt the ICA and HTTP communication between the MetaFrame XP server and the server running the Web Interface, combined with encryption of the HTTP communication between the Web browser and the Web server.

Sample Deployment A - Using SSL Relay

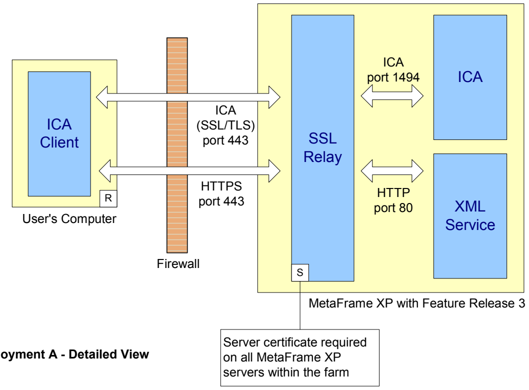
The MetaFrame XP servers in sample deployment A are running MetaFrame XP Server for Windows with Feature Release 3, on Microsoft Windows Server 2003 with Terminal Services. Users in deployment A are running the ICA (Program Neighborhood) Client for Win32, Version 7.0.



Sample Deployment A - SSL Relay

How the Components Interact

You use TLS/SSL to secure the connection between an ICA Client and the MetaFrame XP server. To do this, you deploy TLS/SSL-enabled ICA Clients and configure SSL Relay on the MetaFrame XP server.



Sample Deployment A - Detailed View

This deployment provides end-to-end encryption of the communication between the ICA Client and the MetaFrame XP server. Both SSL Relay and the appropriate server certificate must be installed and configured on each MetaFrame XP server within the server farm.

The SSL Relay operates as an intermediary in the communications between the ICA Client and the XML service at each MetaFrame XP server. Each client authenticates the SSL Relay by checking the SSL Relay's server certificate against a list of trusted certificate authorities. After this authentication, the client and SSL Relay negotiate requests in encrypted form. The SSL Relay decrypts the requests and passes them to the MetaFrame XP server. When returning the information to the client, the MetaFrame XP server sends all information through the SSL Relay, which encrypts the data and forwards it to the client to be decrypted. Message integrity checks verify each communication has not been tampered with.

FIPS 140 Validation

In sample deployment A, the MetaFrame XP Server for Windows with Feature Release 3 SSL Relay uses the Microsoft Cryptographic Service Providers (CSPs) and associated cryptographic algorithms available in the Microsoft Windows CryptoAPI to encrypt/decrypt communication between client and server. Direct questions regarding the FIPS 140 validation of the CSPs to Microsoft Corporation.

For Microsoft Windows XP and Windows Server 2003, the TLS/SSL Support and Supported Ciphersuites can also be controlled by the Microsoft security option:

- System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing. Refer to Microsoft product documentation for details.

For earlier Microsoft operating systems, see the following Microsoft Knowledge Base articles on the Microsoft support Web site (http://support.microsoft.com/):

- Microsoft Knowledge base article Q238268
  "FIPS-Compliant Browser and Web Server for Windows NT 4.0"
- Microsoft Knowledge base article Q245030
  "How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll"

TLS/SSL Support

You can configure MetaFrame XP to use either the Transport Layer Security (TLS) protocol 1.0 or the Secure Sockets Layer (SSL) protocol 3.0. In sample deployment A, the components are configured for TLS.

For details about configuring TLS, see the:

- *Citrix MetaFrame XP Server Administrator's Guide* for Feature Release 3 and the online application help for the SSL Relay Configuration tool. When using the SSL Relay Configuration Tool, ensure that **TLS** is selected at the Connection tab.
- *Citrix ICA Win32, Version 7.0, Client Administrator's Guide*

Supported Ciphersuites

In sample deployment A, you configure MetaFrame XP Server for Windows with Feature Release 3 to use government-approved cryptography to protect "sensitive but unclassified" data. The government ciphersuite is:

RSA_WITH_3DES_EDE_CBC_SHA

For details about configuring government ciphersuites, see the:

- *Citrix MetaFrame XP Server Administrator's Guide* for Feature Release 3 and the online application help for the SSL Relay Configuration tool. When using the SSL Relay Configuration Tool, ensure that only **GOV** is selected at the Ciphersuite tab.
- *Citrix ICA Win32, Version 7.0, Client Administrator's Guide*

Certificates and Certificate Authorities

Citrix products use standard Public Key Infrastructure (PKI) as a framework and trust infrastructure. In sample deployment A, you configure a separate server certificate for each MetaFrame XP server on which you use SSL Relay. A root certificate is required for each client. For further details, see the *Citrix MetaFrame XP Server Administrator's Guide* for Feature Release 3.

Smart Card Support

In sample deployment A, you can configure MetaFrame XP Server for Windows with Feature Release 3 to provide a smart card logon. To do this, you must configure authentication using the Microsoft Active Directory and use the Microsoft Certificate Authority. For more information, see the latest version of the *Advanced Concepts Guide for MetaFrame XP*, available from the Citrix Web site.

ICA Clients

The Citrix ICA (Program Neighborhood) Client for Win32 is used in sample deployment A. For details concerning the security features and capabilities of Citrix ICA Clients, see "ICA Clients" on page 13.

Sample Deployment B - Using Secure Gateway (Single-Hop)

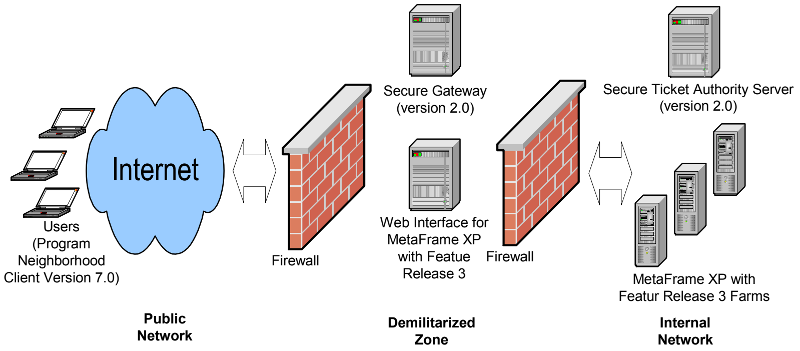
The MetaFrame XP server in sample deployment B is running MetaFrame XP Server for Windows with Feature Release 3 on Microsoft Windows Server 2003 with Terminal Services. Citrix SSL Relay is enabled on the MetaFrame XP server.

The server running the Web Interface in sample deployment B comprises the Web Interface for MetaFrame XP with Feature Release 3, on Microsoft Windows Server 2003, with Microsoft Internet Information Services Version 6.0 or later.

The Secure Gateway in sample deployment B is running on Microsoft Windows Server 2003.

The Secure Ticket Authority in sample deployment B is running on Microsoft Windows Server 2003.

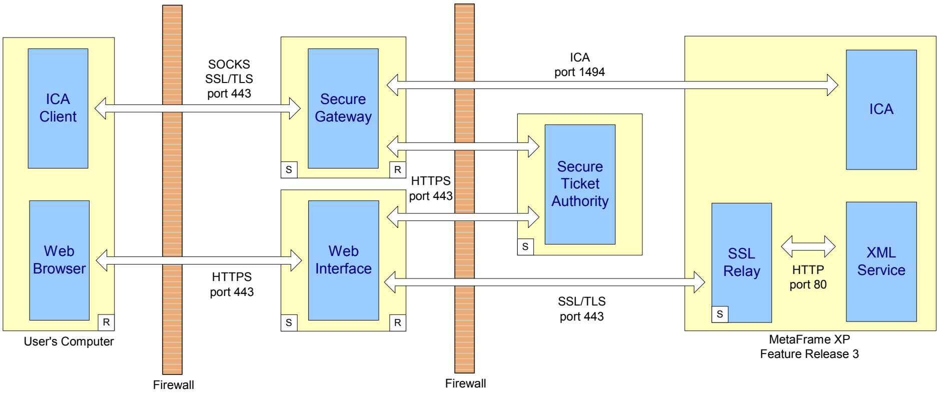
Users in deployment B are running a TLS-enabled Web browser and the Citrix ICA (Program Neighborhood) Client for Win32, Version 7.0.



Deployment B - Secure Gateway

How the Components Interact

You use TLS to secure the connection between an ICA Client and the Secure Gateway. To do this, you deploy TLS/SSL-enabled ICA Clients and deploy the Secure Gateway at the network perimeter, typically in a demilitarized zone (DMZ). You secure the connection between the Web browser and the Web Interface using HTTPS. Additionally, you secure communication between the Web Interface and the Secure Ticket Authority using HTTPS and the Web Interface and MetaFrame XP using TLS.



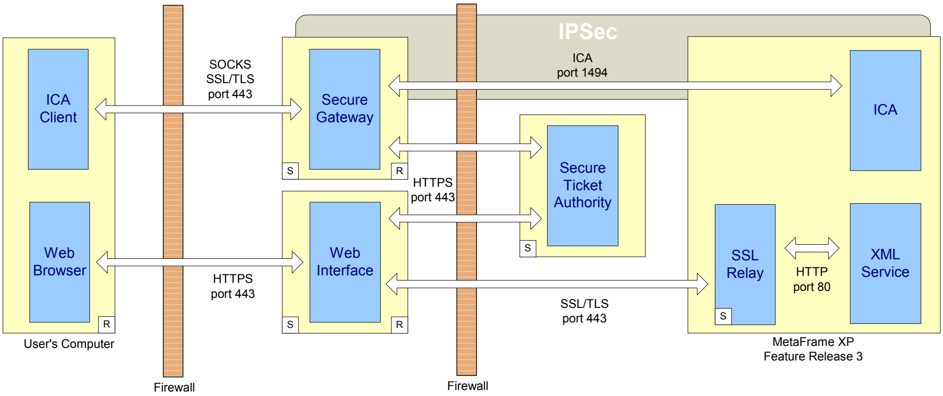
Sample Deployment B.1 - Detailed View

In sample deployment B, the Secure Gateway removes the need to publish the addresses of every MetaFrame XP server, and allows a single point of encryption and access to the Citrix servers. It does this by providing a gateway that is separate from the MetaFrame XP servers and reduces the issues for firewall traversal to a widely accepted port for ICA traffic in and out of firewalls.

Set against the increased scalability of sample deployment B is the fact that ICA communication is encrypted only between the client and the gateway. ICA communication between the gateway and MetaFrame XP servers is not encrypted.

Note that the SSL Relay in Sample Deployment B.1 is used to encrypt communication between the Web Interface and the XML Service at the MetaFrame XP server. The Secure Gateway communicates with MetaFrame XP directly (the SSL Relay is not used for Secure Gateway to MetaFrame XP server communication).

To achieve FIPS 140, you can secure the communication between the Secure Gateway and MetaFrame XP using IPSec. This is illustrated in the next diagram.



Sample Deployment B.2 - Detailed View (IPSec)

IPSec

To enable IPSec to secure communication between the Secure Gateway and MetaFrame XP, you must configure IPSec for the following servers:

- Secure Gateway
- All MetaFrame XP servers

IPSec is configured using the Local Security Settings (IP Security Policies) for each server. IPSec can be configured on Windows 2000 (or later) Servers. In deployment B, IPSec is enabled on the required servers and the security method is configured for 3DES encryption and SHA-1 integrity to meet FIPS 140 requirements.

FIPS 140 Validation

In sample deployment B, the MetaFrame XP Server for Windows with Feature Release 3 SSL Relay uses the Microsoft Cryptographic Service Providers (CSPs) and associated cryptographic algorithms available in the Microsoft Windows CryptoAPI to encrypt/decrypt communication between client and server. Direct questions regarding the FIPS 140 validation of the CSPs to Microsoft Corporation.

For Microsoft Windows XP and Windows Server 2003, the TLS/SSL Support and Supported Ciphersuites can also be controlled by the Microsoft security option:

- System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing. Refer to Microsoft product documentation for details.

For earlier Microsoft operating systems, see the following Microsoft Knowledge Base articles on the Microsoft support Web site (http://support.microsoft.com/):

- Microsoft Knowledge base article Q238268
  "FIPS-Compliant Browser and Web Server for Windows NT 4.0"
- Microsoft Knowledge base article Q245030
  "How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll"

TLS/SSL Support

In sample deployment B, you can configure Secure Gateway 2.0 and the Web Interface to use either the Transport Layer Security (TLS) protocol 1.0 or the Secure Sockets Layer (SSL) protocol 3.0. In sample deployment B, the components are configured for TLS.

For details about configuring TLS, see the:

- *Web Interface for MetaFrame XP with Feature Release 3 Administrator's Guide*
- *Secure Gateway, Version 2.0, Administrator's Guide*
- *Citrix ICA Win32, Version 7.0, Client Administrator's Guide*

Supported Ciphersuites

In sample deployment B, you configure Secure Gateway Version 2.0 and the Web Interface to use government-approved cryptography to protect "sensitive but unclassified" data. The government ciphersuite is:

RSA_WITH_3DES_EDE_CBC_SHA

For details about configuring government ciphersuites, see the:

- *Secure Gateway, Version 2.0, Administrator's Guide*
- *Citrix ICA Win32, Version 7.0, Client Administrator's Guide*

Certificate Authorities

Citrix products use standard Public Key Infrastructure (PKI) as a framework and trust infrastructure. In sample deployment B, you configure one server certificate on the Secure Gateway, and one on the Web Interface. You also configure a certificate on each MetaFrame XP server. For further details, see the relevant Administrator's Guides.

Smart Card Logon

In sample deployment B, you can configure MetaFrame XP Server for Windows with Feature Release 3 to provide a smart card logon. To do this, you must configure authentication using the Microsoft Active Directory and use the Microsoft Certificate Authority.

For more information, see the latest version of the *Advanced Concepts Guide for MetaFrame XP* available from the Citrix Web site.

ICA Clients

The Citrix ICA (Program Neighborhood) Client for Win32 is used in sample deployment B.

For details about the security features and capabilities of Citrix ICA Clients, see "ICA Clients" on page 13.

Sample Deployment C - Using Secure Gateway (Double Hop)

The MetaFrame XP server in sample deployment C is running MetaFrame XP Server for Windows with Feature Release 3 on Microsoft Windows Server 2003 with Terminal Services. Citrix SSL Relay is enabled on the MetaFrame XP server.

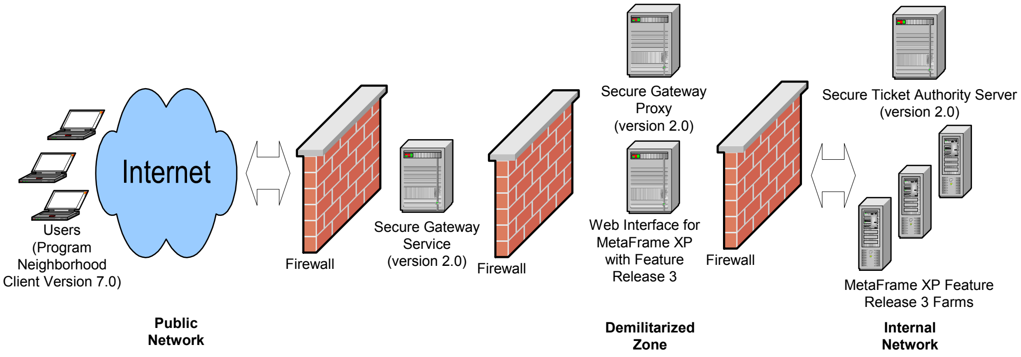
The server running the Web Interface in sample deployment C comprises the Web Interface for MetaFrame XP with Feature Release 3, on Microsoft Windows Server 2003, with Microsoft Internet Information Services Version 6.0 or later.

The Secure Gateway Service in sample deployment C is running on Microsoft Windows Server 2003.

The Secure Gateway Proxy in sample deployment C is running on Microsoft Windows Server 2003.

The Secure Ticket Authority in sample deployment C is running on Microsoft Windows Server 2003.

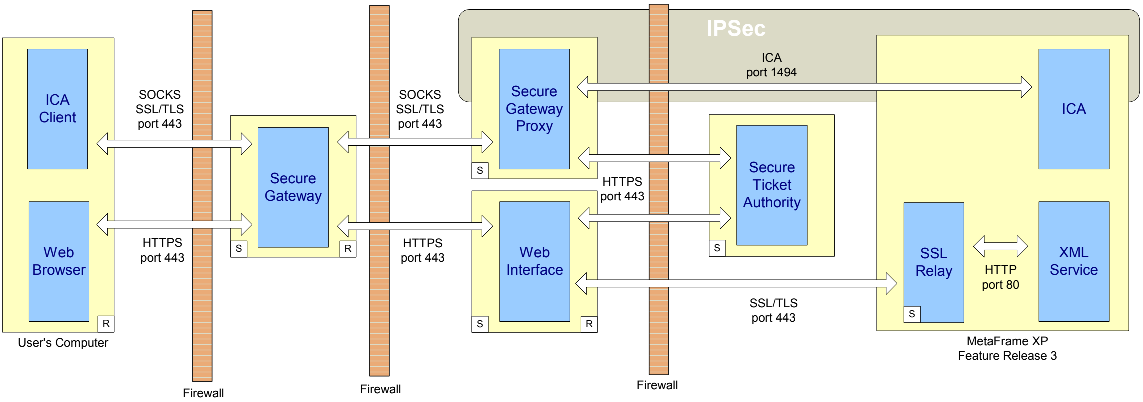
Users in deployment C are running a TLS-enabled Web browser and the Citrix ICA (Program Neighborhood) Client for Win32, Version 7.0.


Internet
Users (Program Neighborhood Client Version 7.0)
Firewall
Secure Gateway Service (version 2.0)
Firewall
Secure Gateway Proxy (version 2.0)
Web Interface for MetaFrame XP with Feature Release 3
Firewall
Secure Ticket Authority Server (version 2.0)
MetaFrame XP Feature Release 3 Farms
Public Network
Demilitarized Zone
Internal Network

Deployment C - Secure Gateway (double hop) and IPSEC

How the Components Interact

You use TLS to secure the connection between an ICA Client and the Secure Gateway. To do this, you deploy TLS/SSL-enabled ICA Clients and deploy the Secure Gateway at the network perimeter, typically in a demilitarized zone (DMZ).



Sample Deployment C - Detailed View

In sample deployment C, the Secure Gateway removes the need to publish the addresses of every MetaFrame XP server and allows a single point of encryption and access to the Citrix servers. It does this by providing a gateway that is separate from the MetaFrame XP servers and reduces the issues for firewall traversal to a widely accepted port for ICA traffic in and out of firewalls.

To achieve FIPS 140, you can secure communication between the Secure Gateway Proxy and MetaFrame XP servers using IPSec.

IPSec

To enable IPSec to secure communication between the Secure Gateway Proxy and MetaFrame XP, you must configure IPSec for the following servers:

- Secure Gateway Proxy
- All MetaFrame XP servers

IPSec is configured using the Local Security Settings (IP Security Policies) for each server. IPSec can be configured on Windows 2000 (or later) Servers. In deployment C, IPSec is enabled on the required servers and the security method is configured for 3DES encryption and SHA-1 integrity to meet FIPS 140 requirements.

FIPS 140 Validation

In sample deployment C, the MetaFrame XP Server for Windows with Feature Release 3 SSL Relay uses the Microsoft Cryptographic Service Providers (CSPs) and associated cryptographic algorithms available in the Microsoft Windows CryptoAPI to encrypt/decrypt communication between client and server. Direct questions regarding the FIPS 140 validation of the CSPs to Microsoft Corporation.

For Microsoft Windows XP and Windows Server 2003, the TLS/SSL Support and Supported Ciphersuites can also be controlled by the Microsoft security option:

- System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing. Refer to Microsoft product documentation for details.

For earlier Microsoft operating systems, see the following Microsoft Knowledge base articles on the Microsoft support Web site (http://support.microsoft.com/):

- Microsoft Knowledge base article Q238268
  “FIPS-Compliant Browser and Web Server for Windows NT 4.0”
- Microsoft Knowledge base article Q245030
  “How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll”

TLS/SSL Support

In sample deployment C, you can configure Secure Gateway 2.0 and the Web Interface to use either the Transport Layer Security (TLS) protocol 1.0 or the Secure Sockets Layer (SSL) protocol 3.0. In sample deployment C, the components are configured for TLS.

For details about configuring TLS, see the:

- *Web Interface for MetaFrame XP with Feature Release 3 Administrator’s Guide*
- *Secure Gateway, Version 2.0, Administrator’s Guide*
- *Citrix ICA Win32, Version 7.0, Client Administrator’s Guide*

Supported Ciphersuites

In sample deployment C, you configure Secure Gateway and Secure Gateway Proxy Version 2.0, and the Web Interface to use government-approved cryptography to protect “sensitive but unclassified” data. The government ciphersuite is:

RSA_WITH_3DES_EDE_CBC_SHA

For details about configuring government ciphersuites, see the:

- *Web Interface for MetaFrame XP with Feature Release 3 Administrator's Guide*
- *Secure Gateway, Version 2.0, Administrator's Guide*
- *Citrix ICA Win32, Version 7.0, Client Administrator's Guide*

Certificate Authorities

Citrix products use standard Public Key Infrastructure (PKI) as a framework and trust infrastructure. In sample deployment C, you configure one server certificate on the Secure Gateway, one on Secure Gateway Proxy, and one on the Web Interface. You also configure a certificate on each MetaFrame XP server. For further details, see the relevant Administrator's Guides.

Smart Card Logon

Smart card authentication is not supported in deployment C. It is not possible to configure smart card support where the Secure Gateway is positioned between the clients and the Web Interface.

For more information, see the *Secure Gateway, Version 2.0, Administrator's Guide.*

ICA Clients

The Citrix ICA (Program Neighborhood) Client for Win32 is used in sample deployment C.

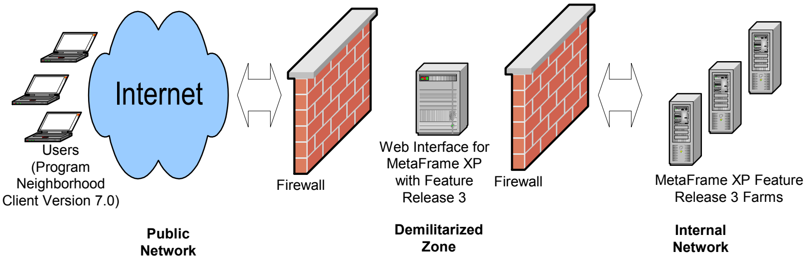
For details about the security features and capabilities of Citrix ICA Clients, see “ICA Clients” on page 13.

Sample Deployment D - Using SSL Relay and the Web Interface

The MetaFrame XP server in sample deployment D is running MetaFrame XP Server for Windows with Feature Release 3 on Microsoft Windows Server 2003 with Terminal Services. Citrix SSL Relay is enabled on the MetaFrame XP server.

The server running the Web Interface in sample deployment D comprises the Web Interface for MetaFrame XP with Feature Release 3 on Microsoft Windows Server 2003, with Microsoft Internet Information Services Version 6.0 or later.

Users in deployment D are running a TLS-enabled Web browser and the Citrix ICA (Program Neighborhood) Client for Win32, Version 7.0.


Internet
Users (Program Neighborhood Client Version 7.0)
Firewall
Web Interface for MetaFrame XP with Feature Release 3
Firewall
MetaFrame XP Feature Release 3 Farms
Public Network
Demilitarized Zone
Internal Network

Sample Deployment D - SSL Relay and the Web Interface

How the Components Interact

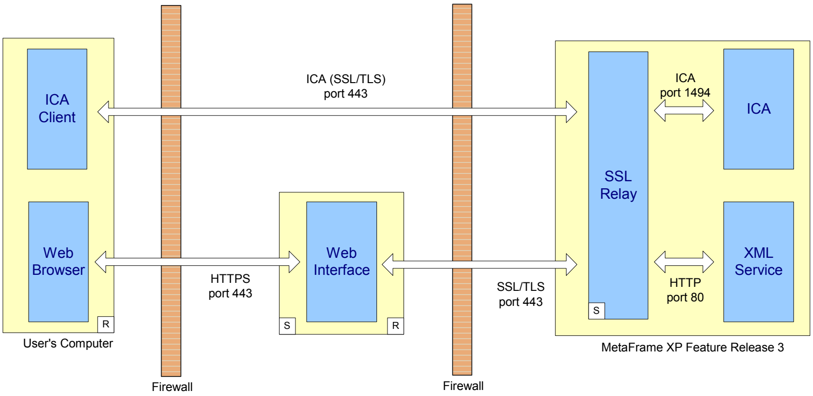
In sample deployment D, the DMZ is divided into two segments. The Secure Gateway Service is located in the first-hop of the DMZ. The Web Interface and Secure Gateway Proxy are located in the second-hop of the DMZ. Users connect to the Secure Gateway server in the first-hop DMZ.

In sample deployment D, you secure the connection between the user's Web browser and the Web Interface using HTTPS. You secure the connection between the Web Interface and the SSL Relay at the MetaFrame XP server using TLS.

The connection between the user's ICA Client and the SSL Relay at the MetaFrame XP server is secured using TLS.

The SSL Relay operates as an intermediary in the communications between the ICA Clients, the Web Interface, and the XML Service at each MetaFrame XP server. Each client authenticates the SSL Relay by checking the SSL Relay's server certificate against a list of trusted certificate authorities. After this authentication, the client and SSL Relay negotiate requests in encrypted form. The SSL Relay decrypts the requests and passes them to the MetaFrame XP server. When returning the information to the client, the MetaFrame XP server sends all information through the SSL Relay, which encrypts the data and forwards it to the client to be decrypted. Message integrity checks verify each communication has not been tampered with.

The following diagram shows the interaction of these components:



Sample Deployment D - Detailed View

FIPS 140 Validation

In sample deployment D, the MetaFrame XP Server for Windows with Feature Release 3 SSL Relay uses the Microsoft Cryptographic Service Providers (CSPs) and associated cryptographic algorithms available in the Microsoft Windows CryptoAPI to encrypt/decrypt communication between client and server. Direct questions regarding the FIPS 140 validation of the CSPs to Microsoft Corporation.

For Microsoft Windows XP and Windows Server 2003, the TLS/SSL Support and Supported Ciphersuites can also be controlled by the Microsoft security option:

- System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing. Refer to Microsoft product documentation for details.

For earlier Microsoft operating systems, see the following Microsoft Knowledge base articles on the Microsoft support Web site (http://support.microsoft.com/):

- Microsoft Knowledge base article Q238268
  “FIPS-Compliant Browser and Web Server for Windows NT 4.0”
- Microsoft Knowledge base article Q245030
  “How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll”

TLS/SSL Support

In sample deployment D, you can configure MetaFrame XP Server for Windows with Feature Release 3 SSL Relay and the Web Interface to use either the Transport Layer Security (TLS) protocol 1.0 or the Secure Sockets Layer (SSL) protocol 3.0. In sample deployment D, the components are configured for TLS.

For details about configuring TLS, see the:

- *Citrix MetaFrame XP Server Administrator’s Guide* for Feature Release 3 and the online application help for the SSL Relay Configuration tool. When using the SSL Relay Configuration Tool, ensure that **TLS** is selected at the Connection tab.
- *Web Interface for MetaFrame XP with Feature Release 3 Administrator’s Guide*
- *Citrix ICA Win32, Version 7.0, Client Administrator’s Guide*

Supported Ciphersuites

In sample deployment D, you configure the MetaFrame XP Server SSL Relay and the Web Interface to use government-approved cryptography to protect “sensitive but unclassified” data. The government ciphersuite is:

RSA_WITH_3DES_EDE_CBC_SHA

For details about configuring government ciphersuites, see the:

- *Citrix MetaFrame XP Server Administrator’s Guide* for Feature Release 3 and the online application help for the SSL Relay Configuration tool. Using the SSL Relay Configuration Tool, ensure that only **GOV** is selected at the Ciphersuite tab.
- *Web Interface for MetaFrame XP with Feature Release 3 Administrator’s Guide*
- *Citrix ICA Win32, Version 7.0, Client Administrator’s Guide*

Certificate Authorities

Citrix products use standard Public Key Infrastructure (PKI) as a framework and trust infrastructure. In sample deployment D, you configure a separate server certificate for each MetaFrame XP server on which you use SSL Relay. For further details, see the *Citrix MetaFrame XP Server Administrator's Guide* for Feature Release 3.

Smart Card Logon

In sample deployment D, you can configure MetaFrame XP Server for Windows with Feature Release 3 to provide a smart card logon. To do this, you must configure authentication using the Microsoft Active Directory and use the Microsoft Certificate Authority.

For more information, see the latest version of the *Advanced Concepts Guide for MetaFrame XP* available from the Citrix Web site.

ICA Clients

The Citrix ICA (Program Neighborhood) Client for Win32 is used in sample deployment D. For details about the security features and capabilities of Citrix ICA Clients, see "ICA Clients" on page 13.